KDDI R&D LABS

暗号プロトコルに関する評価実証実験結果

株式会社 KDDI 研究所
情報セキュリティグループ
太田 陽基

KDDI 研独自ツールによる評価
（KDDI 研究所）

KDDI 研独自ツール紹介

KDDI R&D LABS

- 基本情報
  - 開発元: 株式会社 KDDI 研究所（日本）
  - ツールタイプ: モデルチェックツール
  - 動作環境: Windows
  - 参考文献: Haruki Ota, Shinsaku Kiyomoto, and Yutaka Miyake, “Fast and Automatic Verification of Authentication and Key Exchange Protocols”
- ツールの特徴
  - GUI により、直感的にプロトコル情報を入力可能。
  - 攻撃モデルを詳細に設定することなく、所望のセキュリティプロパティを選択するだけで、対象となる安全性を検証可能。
  - セキュリティパラメータを設定可能で、データ長や鍵長がセキュリティパラメータに対して十分な長さを有するかを検証可能。
  - 具体的な暗号アルゴリズムを設定可能で、対象となる暗号アルゴリズムが危殆化していないかを検証可能。
  - 評価基準として PAL4 を前提にしているにも関わらず、安全性を高速に検証可能（検証プロセスが止まらなくなることはなく、検証結果を必ず出力）。
- 言語仕様
  - ツール自体は Java アプリケーションであるが、GUI による入出力が可能。

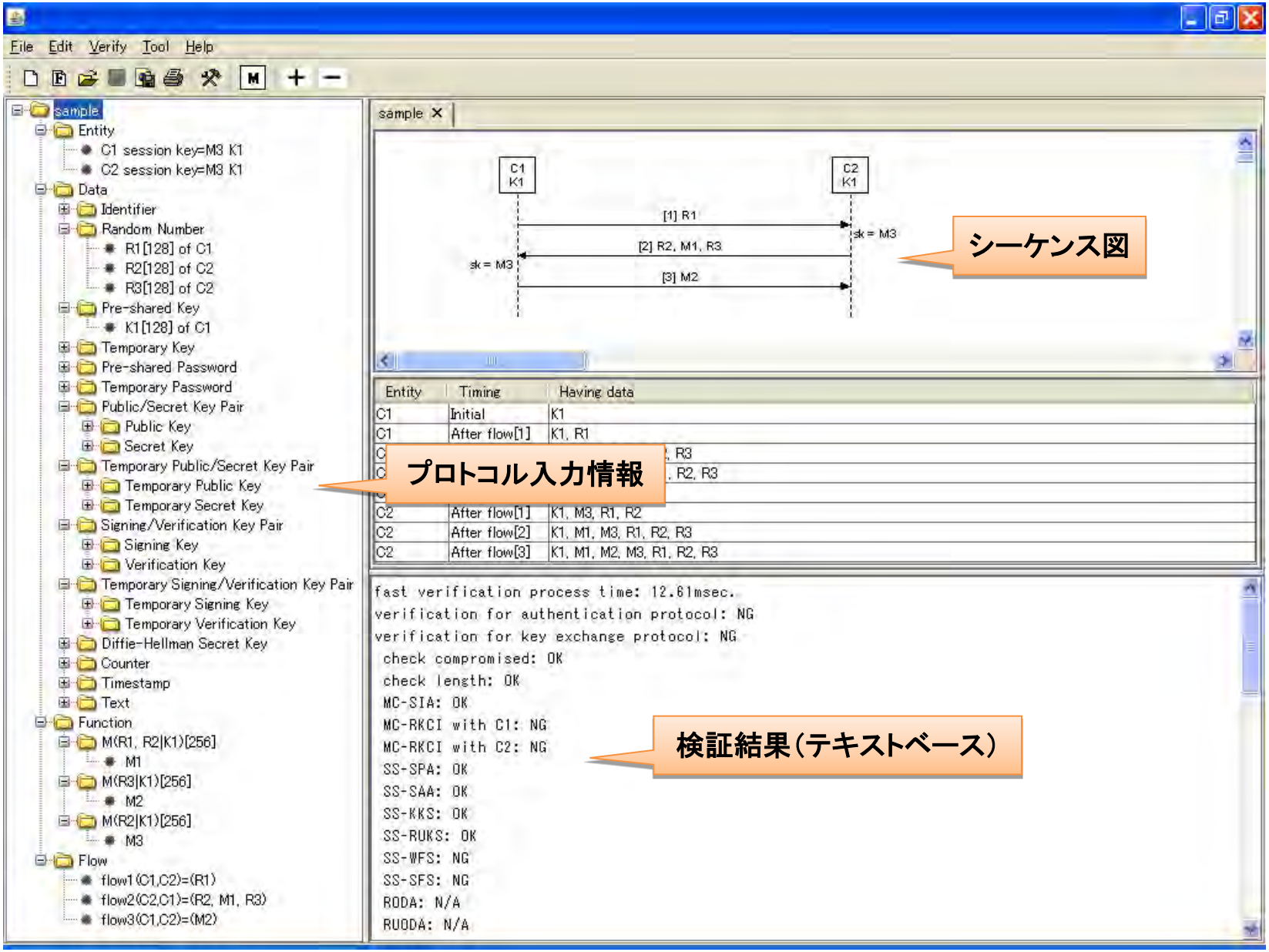
KDDI 研独自ツール紹介（続き）

KDDI R&D LABS

- ユーザーインターフェース
  - 入力
    - GUI により、基本情報、エンティティ、データ、関数、フローなどを入力。
  - 出力
    - 評価結果のみを示したテキスト出力及びプロトコルの入力情報、評価結果、詳細ログを示した GUI 出力（レポートファイル出力）がそれぞれ可能。
    - 入力情報はシーケンス図と表によりわかりやすく表示。
    - 評価結果はプロトコル全体とセキュリティプロパティごとに OK / NG により出力。検証時間、長さと危殆化のチェック結果も出力。
    - セキュリティプロパティが NG になった理由は詳細ログを読み解く必要あり。
- 評価可能性と記述の自由度
  - プロトコル構成、データ・関数の種別、セキュリティプロパティなどが固定されているため、入力可能なプロトコルに対してはモデル記述が容易。
  - 定義されていない入力情報を要するプロトコルの評価不可。評価可能なセキュリティプロパティは以下のとおり。
    - 認証: なりすまし攻撃安全と鍵漏洩なりすまし攻撃安全
    - 鍵交換: 受動的攻撃安全、能動的攻撃安全、既知鍵攻撃安全、未知鍵共有攻撃安全、weak forward secrecy、strong forward secrecy、鍵プライバシ
    - パスワードベース: オフライン辞書攻撃安全と検出不可能なオンライン辞書攻撃安全

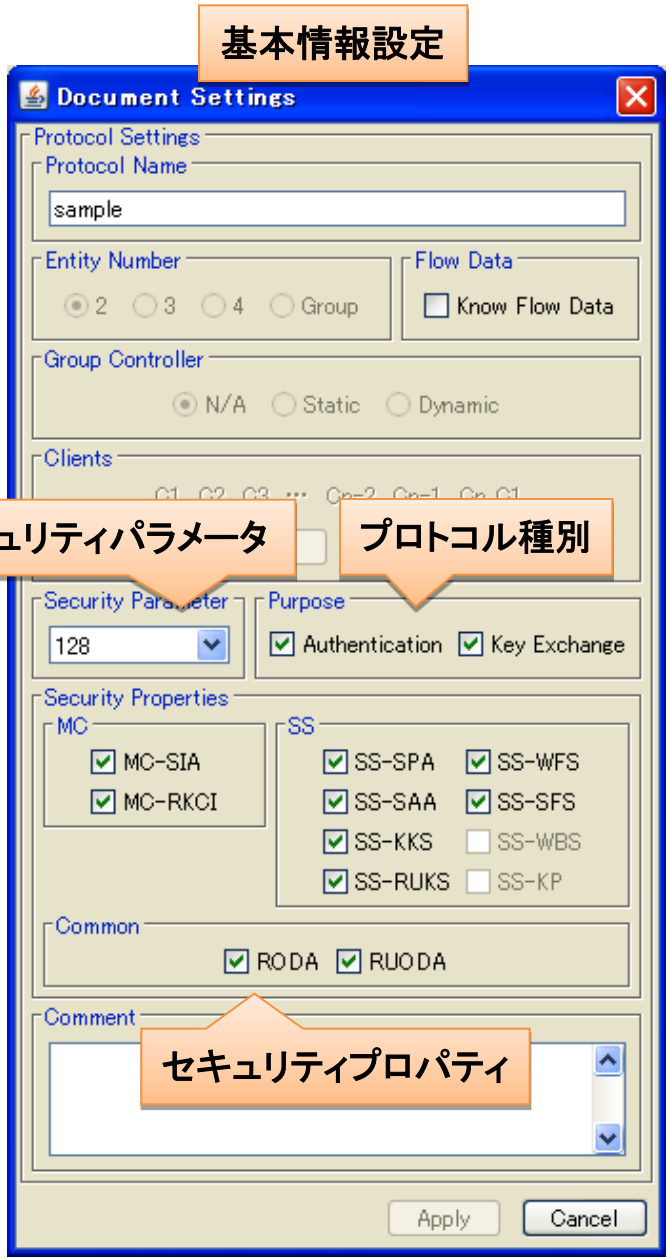
KDDI 研独自ツールの入出力インターフェース

KDDI R&D LABS



KDDI 研独自ツールの入出力インターフェース（続き）

KDDI R&D LABS



KDDI 研独自ツールの入出力インターフェース（続き）

KDDI R&D LABS

レポートファイル

sample プロトコル 評価レポート

プロトコル設定

シーケンス図

名称

sample

セキュリティパラメータ

128

プロトコル入力情報

用途

- 認証プロトコル: 用途あり
- 鍵交換プロトコル: 用途あり

エンティティ

エンティティ	識別子	鍵生成関数	セッション鍵	当初から持っているデータ・関数値
C1	M2(R3|K1)		M3(R2|K1)	K1
C2	M1(R1,R2|K1)		M3(R2|K1)	K1

データ

データ種別	名前	長さ	作成者
乱数	R1	128	C1
	R2	128	C2
	R3	128	C2
事前共有鍵	K1	128	C1

関数

名前	名前（引数｜鍵）	長さ	種別
M1	M1(R1,R2|K1)	256	メッセージ認証コード(MAC)
M2	M2(R3|K1)	256	メッセージ認証コード(MAC)
M3	M3(R2|K1)	256	メッセージ認証コード(MAC)

フロー

名前	同期フロー	送信者	受信者	データ
フロー[1]	フロー1	C1	C2	R1
フロー[2]	フロー2	C2	C1	R2,M1(R1,R2|K1),R3
フロー[3]	フロー3	C1	C2	M2(R3|K1)

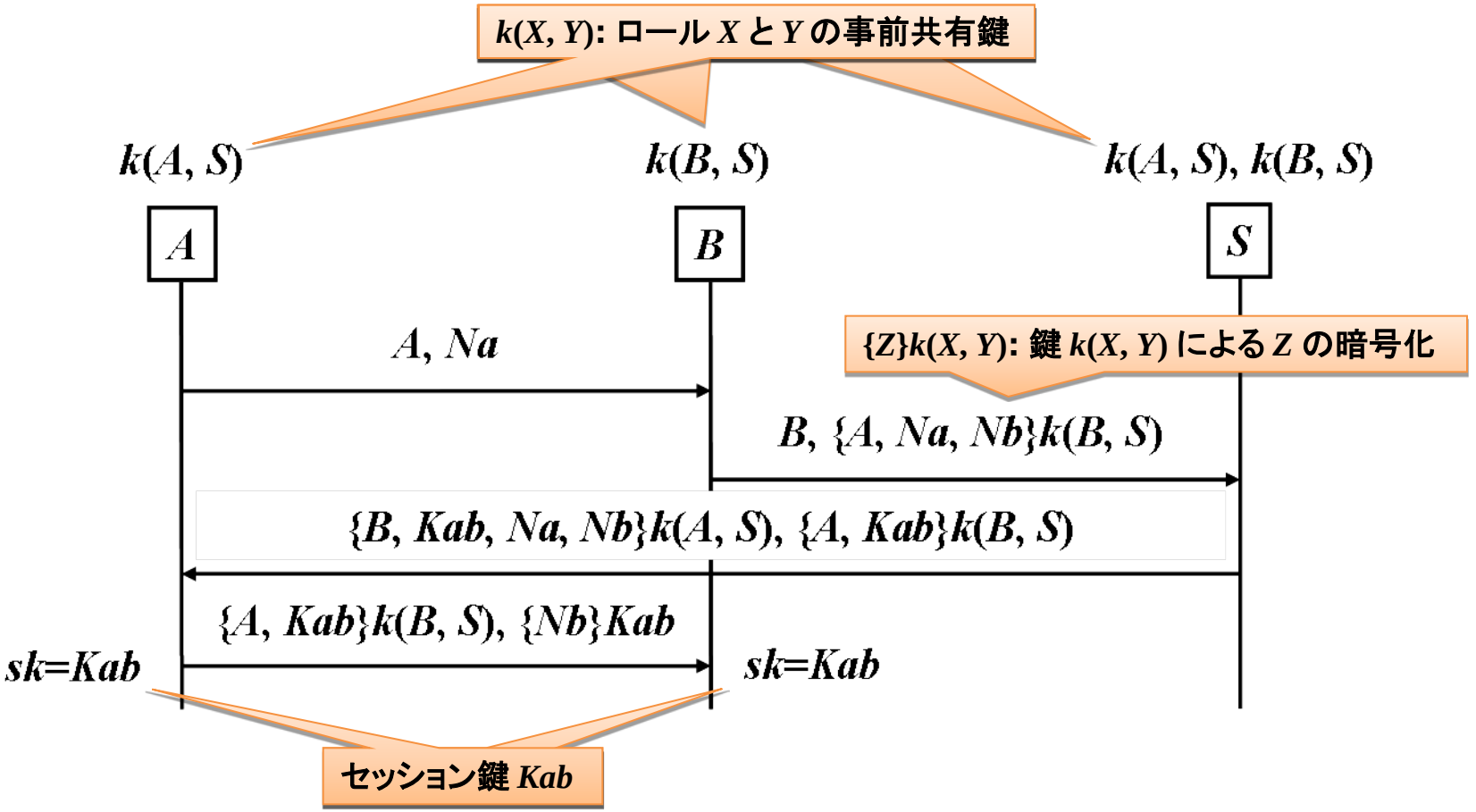
評価結果

メッセージ

```
評価処理時間: 12.61ミリ秒。
認証プロトコルとして評価: NG
鍵交換プロトコルとして評価: NG
 危殆化チェック: OK
 長さチェック: OK
 なりすまし攻撃安全(MC-SIA): OK
 鍵漏洩なりすまし攻撃安全(MC-RKCI with C1): NG
 鍵漏洩なりすまし攻撃安全(MC-RKCI with C2): NG
 受動的攻撃安全(SS-SPA): OK
 能動的攻撃安全(SS-SAA): OK
 既知鍵攻撃安全(SS-KKS): OK
 未知鍵共有攻撃安全(SS-RUKS): OK
 Weak Forward Secrecy(SS-WFS): NG
 Strong Forward Secrecy(SS-SFS): NG
 オフライン辞書攻撃安全(RODA): N/A
 検出不可能なオンライン辞書攻撃安全(RUODA): N/A
  暗号プリミティブ={M1-MAC, M2-MAC, M3-MAC}
  危殆化している関数=[]
  認証子(PAG)={C1-M2, C2-M1}
  鍵生成関数(PKG)={C1-M3, C2-M3}
  セッション鍵={C1-M3, C2-M3}
  セッション鍵生成タイミング={C1→フロー[2]直後, C2→フロー[1]直後}
  一時データ削除タイミング(C1)={R1→フロー[1]直後, R2→フロー[2]直後, R3→フロー[3]直後}
  一時データ削除タイミング(C2)={R1→フロー[2]直後, R2→フロー[2]直後, R3→フロー[2]直後}
  パスワードを含む関数=[]
  引数(SS-SPA)={M3=[]}
  引数(SS-SAA)={M3=[M1]}
  引数(RODA)={}
  引数(PAG)={M1=[], M2=[]}
  その他(SS-SPA)=[]
  その他(SS-SAA)=[]
  その他(RODA)=[]
  その他(PAG)=[]
 [MC-SIA] OK (g,f)={M2=[[g:null, f:M2]]}
   type-status={K1-LLK-SS, M1-TV-PS, M2-TV-PS, M3-TV-SS, R1-TD-PS, R2-TD-PS, R3-TD-PS}
 [MC-SIA] OK (g,f)={M1=[[g:null, f:M1]]}
   type-status={K1-LLK-SS, M1-TV-PS, M2-TV-PS, M3-TV-SS, R1-TD-PS, R2-TD-PS, R3-TD-PS}
 [MC-RKCI with C2] NG (g,f)={M2=[[g:null, f:M2]]}
   type-status={K1-LLK-PS, M1-TV-PS, M2-TV-PS, M3-TV-PS, R1-TD-PS, R2-TD-PS, R3-TD-PS}
 [MC-RKCI with C1] NG (g,f)={M1=[[g:null, f:M1]]}
   type-status={K1-LLK-PS, M1-TV-PS, M2-TV-PS, M3-TV-PS, R1-TD-PS, R2-TD-PS, R3-TD-PS}
 [SS-SPA] OK (g,f)={M3=[[g:null, f:M3]]}
   type-status={K1-LLK-SS, M1-TV-PS, M2-TV-PS, M3-TV-SS, R1-TD-PS, R2-TD-PS, R3-TD-PS}
 [SS-SAA] OK (g,f)={M3=[[g:null, f:M3], [g:M3, f:M1]]}
   type-status={K1-LLK-SS, M1-TV-PS, M2-TV-PS, M3-TV-SS, R1-TD-PS, R2-TD-PS, R3-TD-PS}
 [SS-KKS] OK (g,f)={M3=[[g:null, f:M3], [g:M3, f:M1]]}
   type-status={K1-LLK-SS, M1-TV-PS, M2-TV-PS, M3-TV-SS, R1-TD-PS, R2-TD-PS, R3-TD-PS}
 [SS-RUKS] OK (g,f)={M3=[[g:null, f:M3], [g:M3, f:M1]]}
   type-status={K1-LLK-SS, M1-TV-PS, M2-TV-PS, M3-TV-SS, R1-TD-PS, R2-TD-PS, R3-TD-PS}
 [SS-WFS] NG (g,f)={M3=[[g:null, f:M3], [g:M3, f:M1]]}
   type-status={K1-LLK-PS, M1-TV-PS, M2-TV-PS, M3-TV-PS, R1-TD-PS, R2-TD-PS, R3-TD-PS}
 [SS-SFS] NG (g,f)={M3=[[g:null, f:M3], [g:M3, f:M1]]}
   type-status={K1-LLK-PS, M1-TV-PS, M2-TV-PS, M3-TV-PS, R1-TD-PS, R2-TD-PS, R3-TD-PS}
```

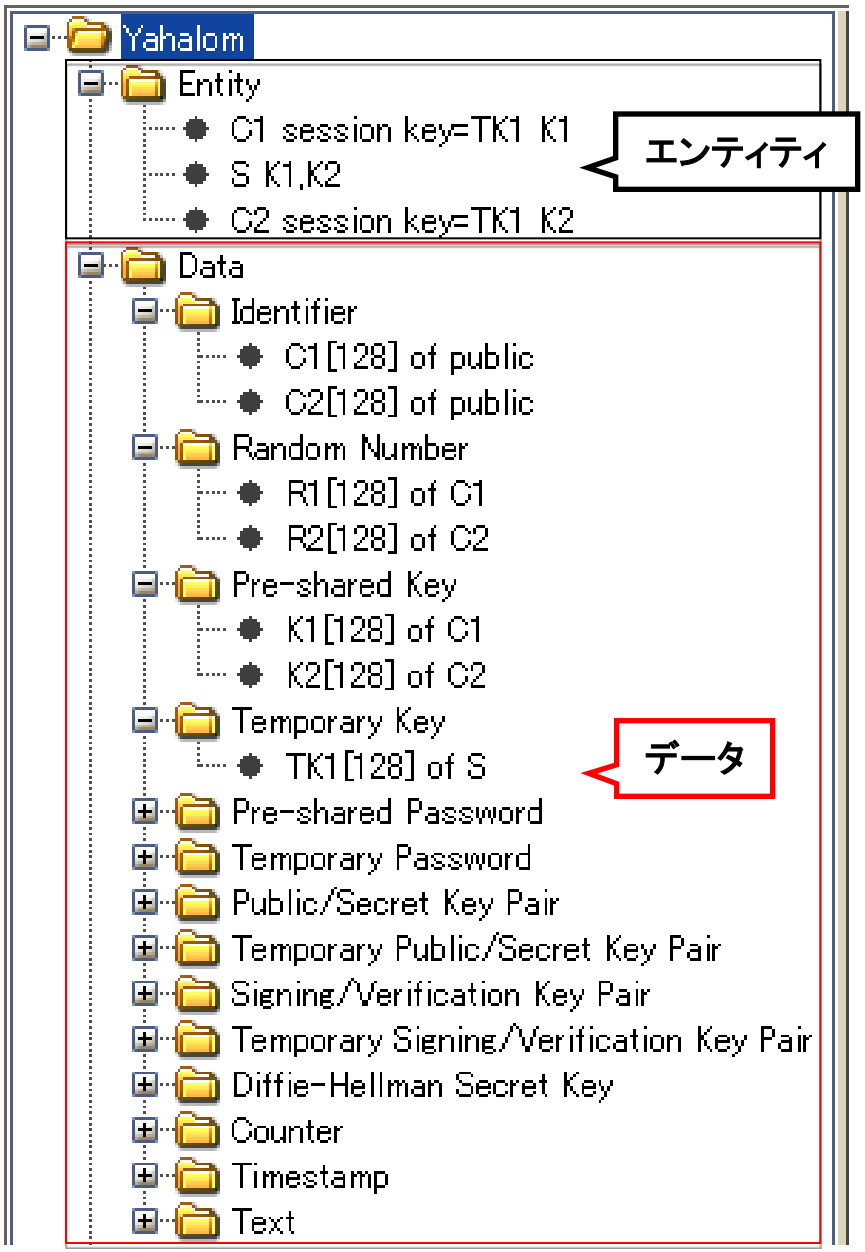
検証結果（GUI ベース）

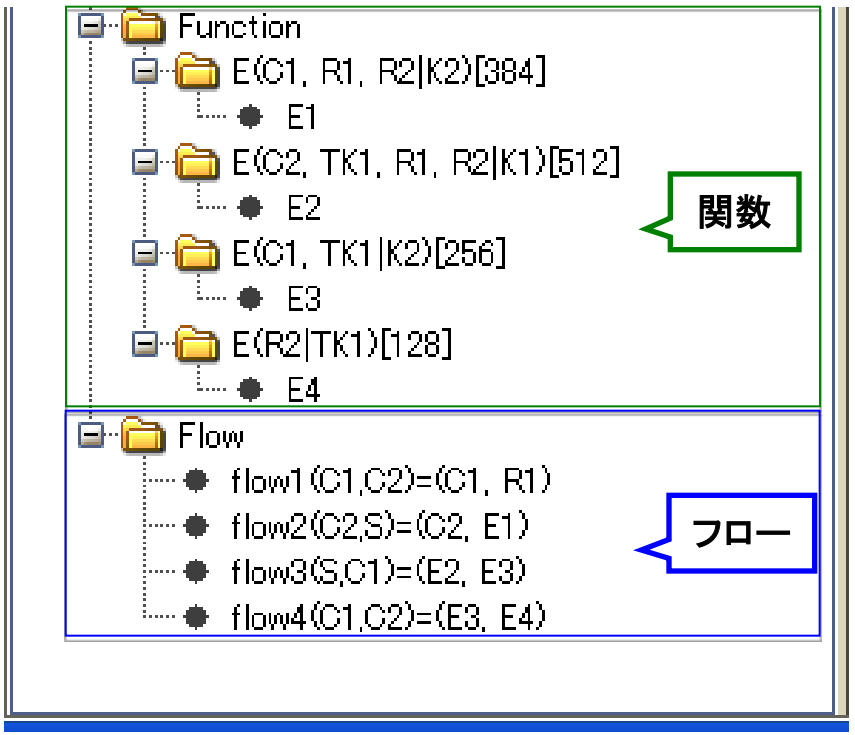
プロトコルの例（Yahalom）

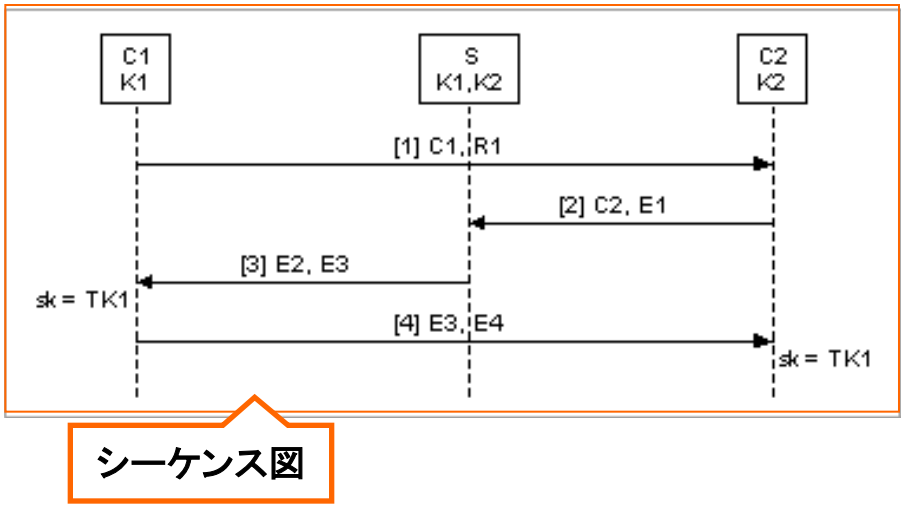


KDDI 研独自ツールによるモデル記述（Yahalom）

KDDI R&D LABS







KDDI 研独自ツールによる検証レポート(Yahalom)

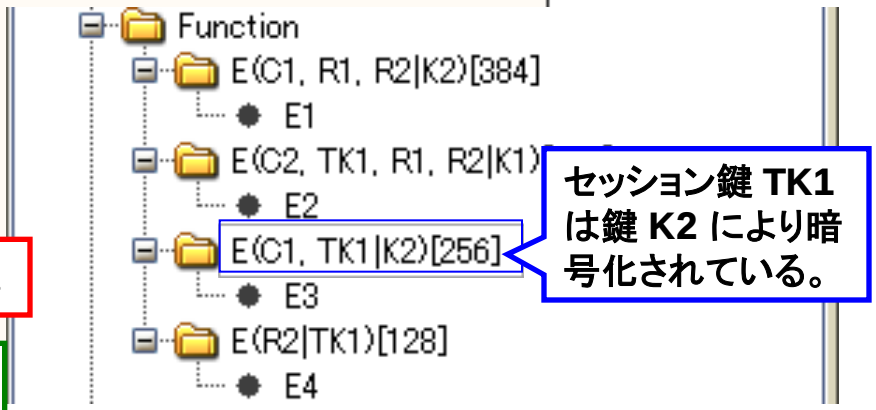
KDDI R&D LABS

評価結果

メッセージ

```
評価処理時間: 15.314ミリ秒。
認証プロトコルとして評価: NG
鍵交換プロトコルとして評価: NG
 危殆化チェック: OK
 長さチェック: OK
 なりすまし攻撃安全(MC-SIA): OK
 鍵漏洩なりすまし攻撃安全(MC-RKCI for C1 with S): NG
 鍵漏洩なりすまし攻撃安全(MC-RKCI for C1 with C2): NG
 鍵漏洩なりすまし攻撃安全(MC-RKCI for S with C1): N/A
 鍵漏洩なりすまし攻撃安全(MC-RKCI for S with C2): N/A
 鍵漏洩なりすまし攻撃安全(MC-RKCI for C2 with C1): OK
 鍵漏洩なりすまし攻撃安全(MC-RKCI for C2 with S): NG
 受動的攻撃安全(SS-SPA): OK
 能動的攻撃安全(SS-SAA): OK
 既知鍵攻撃安全(SS-KKS): OK
 未知鍵共有攻撃安全(SS-RUKS): OK
 Weak Forward Secrecy(SS-WFS): NG
 Strong Forward Secrecy(SS-SFS): NG
 鍵プライバシ(SS-KP): N/A
```

安全でないと判定。



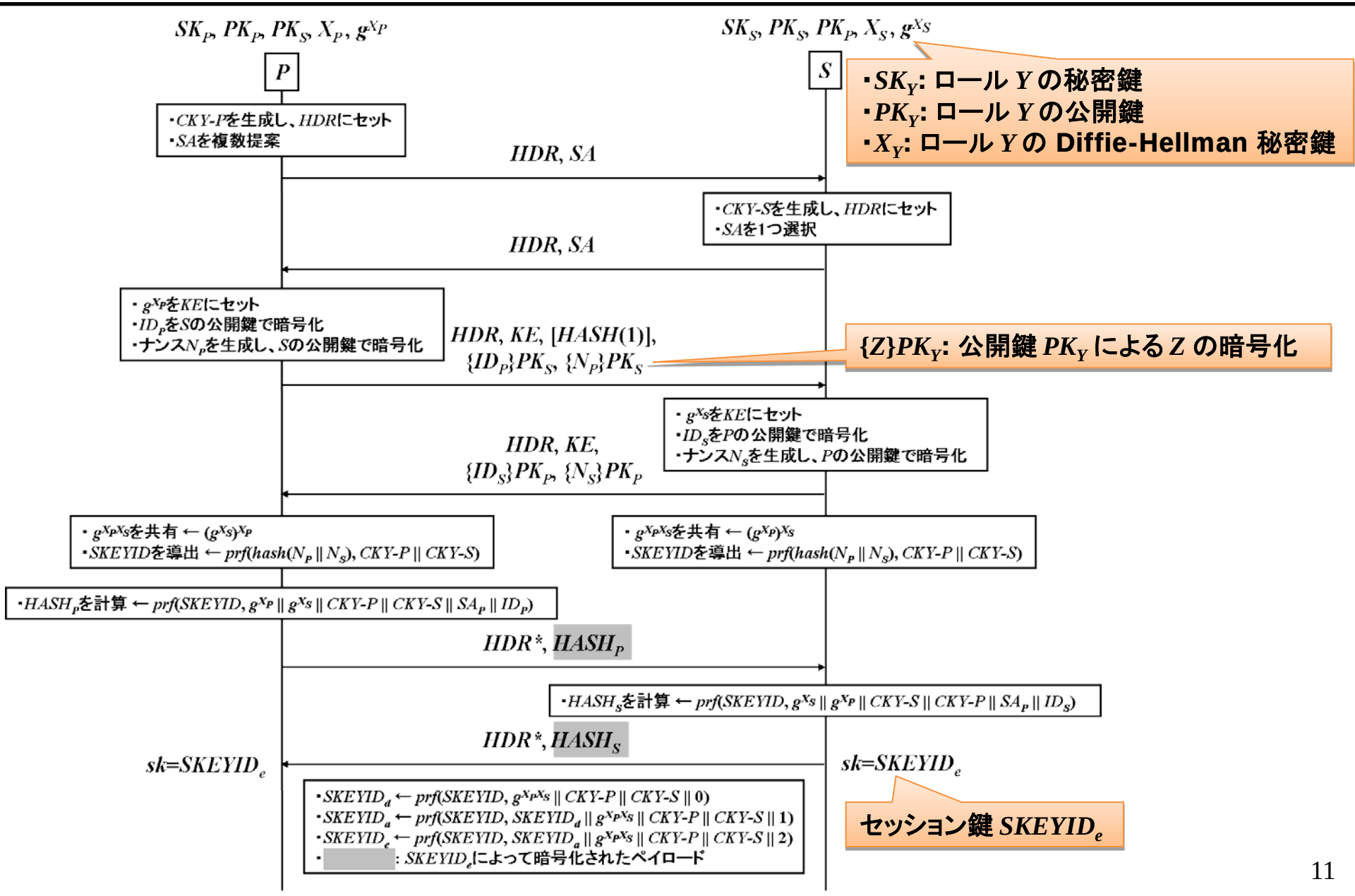
セッション鍵 TK1 は鍵 K2 により暗号化されている。

攻撃者は鍵 K2 を知っているため、セッション鍵 TK1 も得られる。

```
[SS-WFS] NG ( E4], [g:E4, f:E2], [g:E4, f:E3]]}
  type-status={I  P5, E2=IV-PS, E3=TV-PS, E4=TV-PS, C1=ID-PS, C2=ID-PS,
K1=LLK-PS, K2=LLK-PS, TK1=TK-PS, R1=TD-PS, R2=TD-PS}
```

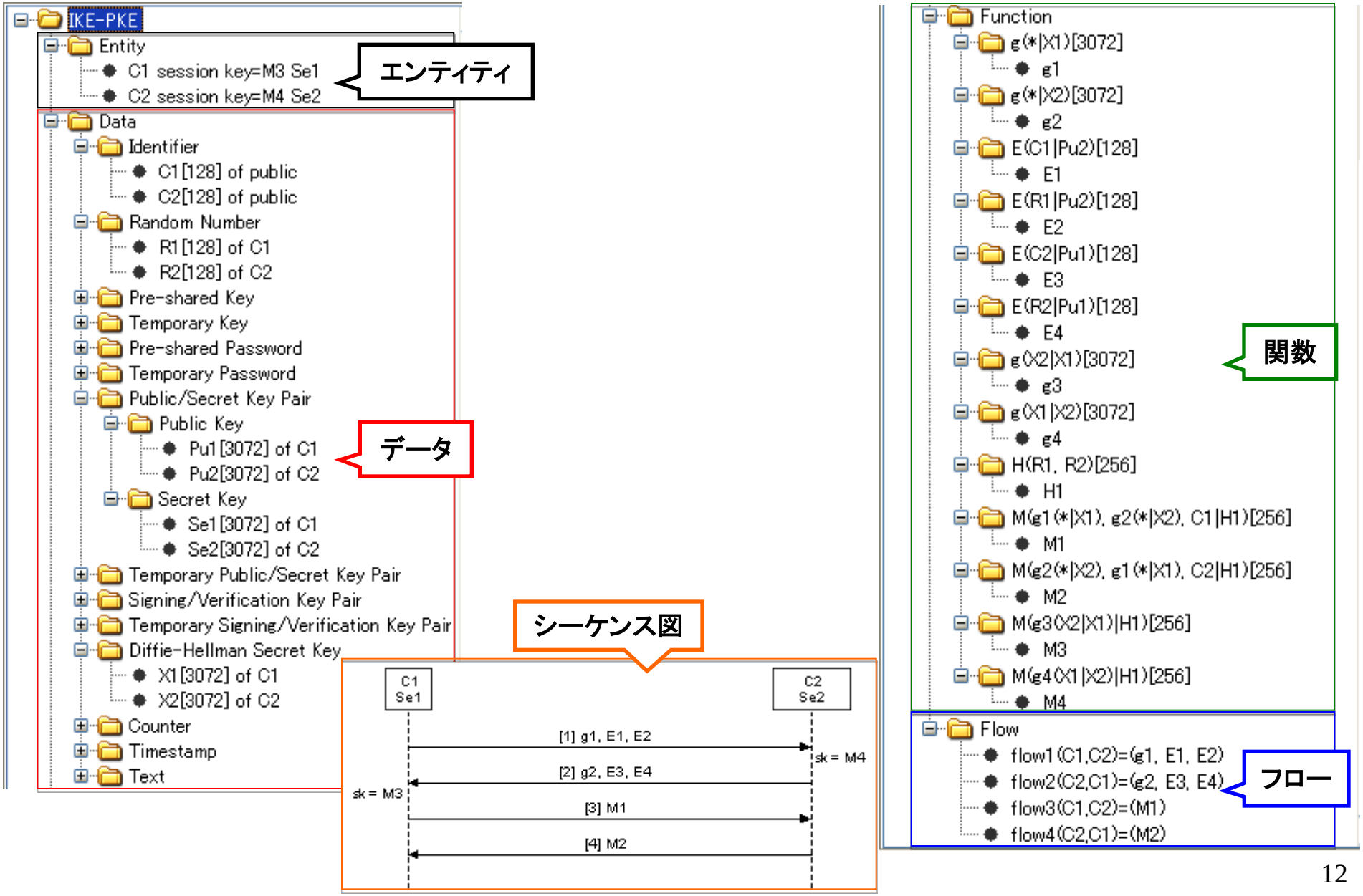
少し複雑なプロトコル（IKE-PKE）

KDDI R&D LABS



KDDI 研独自ツールによるモデル記述（IKE-PKE）

KDDI R&D LABS



KDDI 研独自ツールによる検証レポート(IKE-PKE)

KDDI R&D LABS

評価結果

メッセージ

```
評価処理時間: 22.467ミリ秒。
認証プロトコルとして評価: OK
鍵交換プロトコルとして評価: OK
 危殆化チェック: OK
 長さチェック: OK
 なりすまし攻撃安全(MC-SIA): OK
 鍵漏洩なりすまし攻撃安全(MC-RKCI with C1): OK
 鍵漏洩なりすまし攻撃安全(MC-RKCI with C2): OK
 受動的攻撃安全(SS-SPA): OK
 能動的攻撃安全(SS-SAA): OK
 既知鍵攻撃安全(SS-KKS): OK
 未知鍵共有攻撃安全(SS-RUKS): OK
 Weak Forward Secrecy(SS-WFS): OK
 Strong Forward Secrecy(SS-SFS): OK
```

KDDI 研独自ツールにおいて検証可能なすべての安全性を満足すると判定。

KDDI 研独自ツールに関する知見

KDDI R&D LABS

- プロトコル仕様
  - 仕様の不明確さなどのために、どのように入力されるかに依存して、検証結果が変わる可能性あり。
- モデル記述
  - どの情報を入力すると正しく検証されるのかのノウハウが必要。
  - プロトコル情報のモデル化により、検証結果が変わる可能性あり。
  - モデル化の正当性・妥当性を別途評価する必要あり。
- 評価の実行および結果の解釈
  - 認証子やセッション鍵を設定する必要があり、認証子やセッション鍵が明確でない場合には検証結果が変わる可能性あり。
  - 一部の特殊なプロトコルでは、鍵生成関数や引数などを別途設定しなければならないが、そのノウハウが必要。
  - 検証結果の詳細ログを読み解くにはノウハウが必要であり、安全でないと判定された場合の脆弱性の理解にもノウハウが必要。
  - 検証結果の正当性・妥当性を別途評価する必要あり。

KDDI 研独自ツールに関する知見（続き）

KDDI R&D LABS

- ツールの制約
  - データや関数種別が決まっているので、種別にない情報を入力不可。
  - 「その他の関数」を選択可能であるが、検証結果が正しくない可能性あり。
  - 規定されたセキュリティプロパティ以外の安全性を検証不可で、規定されたセキュリティプロパティ内でも、さらに分類した安全性を検証不可。
  - 2 種類以上の認証子やセッション鍵を設定不可。
  - 長さが明確に定義されている関数の出力値の一部だけを使用するような設定不可。
- その他
  - パスワードベースを除く認証プロトコルでは、2 種類の安全性しかなく、攻撃者モデルを詳細化する必要あり。